CLAIMS:

1. A security server for use in a telecommunications network, the security server configured to:

receive a message;

determine whether the message is from a known source or an unknown source and, depending on a result of the determination, modify the message; and

forward the message within the telecommunications network.

2. A security server according to claim 1, configured to receive a message from outside the telecommunications network.

3. A security server according to claim 1, configured to modify the message by adding a parameter to the message that indicates that the message has come from a known or an unknown source.

4. A security server according to claim 3, wherein the security server is configured to receive a message that includes an identity header and is further configured to add the parameter to the identity header of the message.

5. A security server according to claim 4, wherein the message comprises a SIP message.

6. A security server according to claim 4, wherein the identity header comprises a P-Asserted-Identity.

7. A security server according to claim 1, configured to receive a message that includes an identity header and is further configured to modify the message by removing at least part of the identity header.

8. A security server according to claim 7, configured to detect whether

the identity header is of a particular type and if so to remove at least part of the header.

9. A security server according to claim 7, wherein the message comprises a SIP message.

10. A security server according to claim 8, configured to detect whether the identity header comprises a P-Asserted-Identity type.

11. A security server according to claim 1, wherein the security server is configured to determine whether the message is from a known source or an unknown source by determining whether or not the message has been received via a secure means.

12. A security server according to claim 11, wherein the secure means is a Za interface.

13. A security server according to claim 1, wherein the security server comprises an interrogating call session control function.

14. A network processing element for use in a telecommunications network, the network processing element configured to:

receive a message from another network element;

determine whether the message has been modified and, depending on a result of the determination, perform one or more security checks in respect of the message.

15. A network processing element according to claim 14, configured to determine whether an identity header of the message has been modified by detecting whether the identity header of the message includes an added parameter.

16. A network processing element according to claim 15, wherein the message comprises a SIP message.

17. A network processing element according to claim 15, wherein the identity header comprises a P-Asserted-Identity.

18. A network processing element according to claim 14, configured to determine whether the message has been modified by determining whether all or part an identity header of the message has been removed.

19. A network processing element according to claim 18, wherein the message comprises a SIP message.

20. A network processing element according to claim 18, wherein the identity header comprises a P-Asserted-Identity.

21. A network processing element according to claim 14, that comprises a serving call session control function.

22. A telecommunications network comprising a security server and a network processing element, the security server being configured to:

receive a message;

determine whether the message is from a known source or an unknown source and, depending on a result of the determination, modify the message; and

forward the message to the network processing element.

23. A telecommunications network according to claim 22, wherein the security server is configured to receive a message from outside the telecommunications network.

24. A telecommunications network according to claim 22, wherein the network processing element is configured to:

receive a message forwarded by the security server; and

determine whether the message has been modified and, depending on the result of the determination, perform one or more security checks in respect of the message.

25. A method of performing a security check on a message in a telecommunications network, the method comprising the steps of:

receiving a message;

determining whether the message is from a known source or an unknown source and, depending on a result of the determination, modifying the message; and

forwarding the message within the telecommunications network.

26. A security server for use in a telecommunications network, the security server configured to:

receive a message;

determine whether the message is from a known source or an unknown source; and

forward the message within the communications network in a manner dependent on a result of the determination.

27. A security server according to claim 26, configured to receive the message from outside the telecommunications network.

28. A security server according to claim 26, configured to forward the message without security, if it is determined that the message is from an unknown source.

29. A security server according to claim 26, configured to forward the

message with security, if it is determined that the message is from a known source.

30. A security server according to claim 28, wherein the security comprises a Zb interface.

31. A security server according to claim 26, wherein the message comprises a SIP message.

32. A security server according to claim 26, wherein the security server comprises an interrogating call session control function.

33. A telecommunications network comprising a security server and a network processing element, the security server being configured to:

receive a message;

determine whether the message is from a known source or an unknown source; and

forward the message to the network processing element in a manner dependent on a result of the determination.

34. A telecommunications network according to claim 33, wherein the security server is configured to receive a message from outside the telecommunications network.

35. The telecommunications network according to claim 33, further comprising: an internal security system,

wherein the security server is arranged to forward the message via the internal security system, if it is determined that a message is from a known source, and

wherein the security system is configured to not forward the message via the internal security system, if it is determined that the message is from an unknown source.

36. A telecommunications network according to claim 35, wherein the internal security system comprises a UMTS specified security system.

37. A telecommunications network according to claim 35, wherein the internal security system comprises a Zb interface.

38. A telecommunications network according to claim 33, wherein the message comprises a SIP message.

39. A telecommunications network according to claim 33, wherein the security server is configured to determine whether a message is from a known source or an unknown source by determining whether or not the message has been received via a secure means.

40. A telecommunications network according to claim 39, wherein the secure means comprises a UMTS standard security means.

41. A telecommunications network according to claim 39, wherein the secure means comprises a Za interface.

42. A telecommunications network according to claim 33, wherein the security server comprises an interrogating call session control function.

43. A method of performing a security check on a message in a telecommunications network, the method comprising the steps of:

receiving a message;

determining whether the message is from a known source or an unknown source; and

forwarding the message within the communications network in a manner

dependent on a result of the determination.

44. A security server for use in a telecommunications network, the security server configured to:

receive a message; and

determine whether the message is from a known source or an unknown source and,

depending on a result of the determination, determine a subsequent action to be taken in respect of the message.

45. A method of performing a security check on a message in a telecommunications network, the method comprising the steps of:

receiving a message; and

determining whether the message is from a known source or an unknown source and, depending on a result of a determination, determining a subsequent action to be taken in respect of the message.

46. A security server for use in a telecommunications network, the security server comprising:

receiving means for receiving a message;

determining means for determining whether the message is from a known source or an unknown source and, depending on a result of the determination, modify the message; and

forwarding means for forwarding the message within the telecommunications network.

47. A network processing element for use in a telecommunications network, the network processing element comprising:

receiving means for receiving a message from another network element;

determining means for determining whether the message has been modified

and, depending on a result of the determination, performing one or more security checks in respect of the message.

48. A security server for use in a telecommunications network, the security server comprising:

receiving means for receiving a message;

determining means for determining whether the message is from a known source or an unknown source; and

forwarding means for forwarding the message within the communications network in a manner dependent on a result of the determination.